# DRAFT

**July 2003**
**Version 2.0**
July 14, 2003

MEMORANDUM FOR OFFICE OF THE SECRETARY OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Public Key Infrastructure (PKI) and Public Key Enabling (PKE) Implementation Milestones

References: (a) Department of Defense (DoD) Instruction 8520.aa "Public Key Infrastructure (PKI) and Public Key Enabling (PKE)." date TBD

This memorandum provides milestones and implementation dates for the procedures identified in enclosure 3 of DoD Instruction 8520.aa, Public Key Infrastructure (PKI) and Public Key Enabling (PKE) (reference (a)). Key milestones are identified for completing the DoD PKI and issuing PKI certificates. Milestones also are identified for enabling DoD applications to rely on certificates issued by the DoD PKI and the External Certification Authorities (ECAs). References to DoD Instruction 8520.aa sections are provided in parentheses after each milestone statement shown in table 1.

Since the activation of the DoD PKI in late October 2001 more than two and one half million Common Access Cards (CAC) have been issued. The capacity to issue the CAC continues to increase as Real-time Automated Personnel Identification System (RAPIDS) stations continue to keep pace with the RAPIDS fielding schedule. Fielding of these stations is expected to be completed in August 2003. Based on this August 2003 milestone, all eligible DoD personnel shall be issued PKI certificates on the CAC by October 2003. Contractors and other personnel who are not eligible to be issued DoD PKI certificates may obtain certificates from approved ECAs.

Certificate issuance and other DoD Instruction 8520.aa (reference (a)) requirements are included in the following table along with implementation dates.

Table 1. PKI-PKE Implementation Milestones and Dates

| Milestone | Implementation Dates | | |
|---|---|---|---|
| | Unclassified | Classified (SIPRNet) | Tactical (Unclassified and Classified) |
| Implement a scalable key recovery service for private keys associated with e-mail encryption certificates that supports key history management as well as third party key recovery. (E3.2.5) | Dec 03 | Jun 06 | Oct 06 |
| Issue a primary DoD PKI identity certificate to all eligible users. (E3.2) | Oct 03 | Jun 06 | N/A[1] |
| Enable networks that are required to authenticate users to perform this authentication using certificates issued by the DoD PKI on hardware tokens. (E3.3.1) | Oct 03 | Dec 06 | Dec 06 |
| Enable private web-enabled applications to use DoD-approved (DoD PKI or ECA) certificates for server authentication, integrity, and confidentiality. (E3.3.2.1) | Immediate (Dec 00) | Oct 04 | Oct 06 |
| Enable private web-enabled applications to require client certificate based authentication using DoD-approved (DoD PKI or ECA) certificates. (E3.3.2.2) | Oct 03 | Dec 06 | Dec 06 |
| Implement access control for private web-enabled applications that require access control based on individual identity using appropriate cryptographic techniques based on the identity contained in a DoD-approved (DoD PKI or ECA) certificate. (E3.3.2.3) | Oct 03 | Dec 06 | Dec 06 |
| Support digital signature and encryption capabilities for all E-mail systems using DoD-approved (DoD PKI or ECA) certificates. (E3.3.3) | Oct 03 | Dec 06 | Dec 06 |
| Require E-mail sent to the DoD from external government and private sector entities to be signed using DoD-approved (DoD PKI or ECA) certificates when data integrity, message authenticity, or nonrepudiation are required, and encrypted when it contains sensitive information. (E3.3.3.2) | Oct 03 | Dec 06 | Dec 06 |
| Enable applications other than network login, private web-enabled applications, or email, that use or require the use of public key cryptography to use DoD-approved (DoD PKI or ECA) certificates for server authentication, integrity, and confidentiality and for client certificate based authentication. Legacy applications scheduled for phase-out or replacement by the suspense date may be exempted if warranted by a business case analysis. (E3.3.4) | Oct 07 | Oct 07 | Oct 07 |
| Public key enable other applications as warranted by business case analyses. (E3.3.5) | Oct 07 | Oct 07 | Oct 07 |

To allow for possible CAC issuance delays or the inability of a DoD Component to meet the October 2003 milestones, a grace period not to exceed six months, may be granted at the discretion of the Component Chief Information Officer (CIO). Where the approved grace period cannot be met, a waiver request must be submitted to the Component CIO.

Components should continue to support DoD PKI requirements, both CAC and non-CAC based, for specific programs and mission needs as they arise. As required, DoD Component CIOs may approve waivers to the above dates on a case-by case basis. Waivers shall be granted

[1] *All users must be issued certificates in compliance with the Unclassified and Classified milestone dates.*

only for the minimum length of time required to achieve compliance. Approved waivers shall be reported to the DoD CIO within 15 days of approval.

The DoD remains firmly committed to the implementation of PKI and the enabling of applications to take advantage of the IA security services provided by PKI.

My point of contact for this memorandum is Mr. James Kenneth Osterritter, DoD PKI Action Officer, (703) 602-9985, or e-mail: james.osterritter@osd.mil.

John P. Stenbit
DoD Chief Information Officer